Übungsblatt 13 für Analyse von Algorithmen (16.1.2013)

61.) Man zeige, dass es für jede ungerade natürliche Zahl n, die keine Primzahl ist, ganze Zahlen a, b mit $n = a^2 - b^2$ gibt.

62.) Es sei g eine Primitivwurzel modulo einer ungeraden Primzahl p (d.h. die Restklasse $\overline{g}$ ist ein erzeugendes Element der Gruppe $\mathbb{Z}_p^*$). Man zeige, dass dann g oder $g + p$ ein erzeugendes Element der multiplikative Gruppe $\mathbb{Z}_{p^2}^*$ bildet.

63.) Man untersuche den Aufwand eines Durchlaufs des Miller-Rabin-Tests.

64.) Die Folgen U_n, V_n und L_n sind induktiv definiert:

$$\begin{aligned} &U_0 = 0,\ U_1 = 0,\ U_{n+1} = 4U_n - U_{n-1}, \\ &V_0 = 2,\ V_1 = 4,\ V_{n+1} = 4V_n - V_{n-1}, \\ &L_0 = 4,\ L_{n+1} = L_n^2 - 2. \end{aligned}$$

Man zeige die Identitäten

$$\begin{aligned} V_n &= U_{n+1} - U_{n-1}, \\ U_n &= \left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right)/\sqrt{12}, \\ V_n &= (2+\sqrt{3})^n + (2-\sqrt{3})^n, \\ U_{n+m} &= U_m U_{n+1} - U_{m-1} U_n \\ L_n &= V_{2^n}. \end{aligned}$$

65.) Man zeige weiters $\mathrm{ggT}(U_n, U_{n+1}) = 1$ und $\mathrm{ggT}(U_n, V_n) \leq 2$.